Fortinet FortiGate Virtual Appliance for Microsoft Azure Quick Start Guide

FORTINET FORTIGATE VIRTUAL APPLIANCE FOR MICROSOFT AZURE QUICK START GUIDE

The following section will take you through a step-by-step process in order to deploy Fortinet FortiGate on Azure.

What Is the FortiGate Enterprise Firewall for Azure?

The Fortinet FortiGate Enterprise Firewall offers enterprise-class firewall and network protection for your cloud-based applications and infrastructure across a broad spectrum of potential security threats. Empowered by advanced IPC technology, FortiGate helps to protect against known threats and newly emerging threats through anomaly-based detection that identifies attack behavior profiles rather than specific past exploits. FortiGate delivers complete content and network protection, antivirus, application control, web filtering, and VPN along with advanced features such as an extreme threat database, vulnerability management, and flow-based inspection work, all with the scalability and functionality of Azure.

Why FortiGate on Azure?

Built-in Azure firewalls provide a good baseline level of firewall tools, including a web application firewall; however, when your Azure VNETs are interacting with the open Internet, it is essential to augment these baseline firewall features. FortiGate's advanced threat detection technology helps to identify threats before they are widely known and recognized. The easy-to-use and streamlined FortiGate user interface allows quicker setup with more granular control than many standard web application firewalls. Configuring multiple high-availability options is relatively straightforward. FortiGate provides next-generation firewall functionality, securing the virtual infrastructure while also providing VPN and Internet gateway protection.

The Fortinet FortiGate-VM firewall technology for Azure delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, web filtering, and VPN along with advanced features such as an extreme threat database, vulnerability management, and flow-based inspection work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system is purpose-built for inspection and identification of malware.

The FortiGate Virtual Appliance offers protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system. IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection, which alerts users to any traffic that matches attack behavior profiles.

How to Deploy the Fortigate Next-Generation Firewall in Microsoft Azure Using the Azure Portal and ARM

The FortiGate Next-Generation Firewall for Microsoft Azure is deployed as a virtual machine in Microsoft's Azure cloud (IaaS). You will see in the following sections how to deploy and configure the FortiGate in the Azure Marketplace.

- FortiGate Next-Generation Firewall (BYOL)—This is currently the only licensing model that is supported. Fortinet also offers a 60-day evaluation license.

BEFORE YOU GET STARTED

Before you can begin to deploy the FortiGate Next-Generation Firewall, you will need to make sure the following conditions have been met in order to successfully complete the installation:

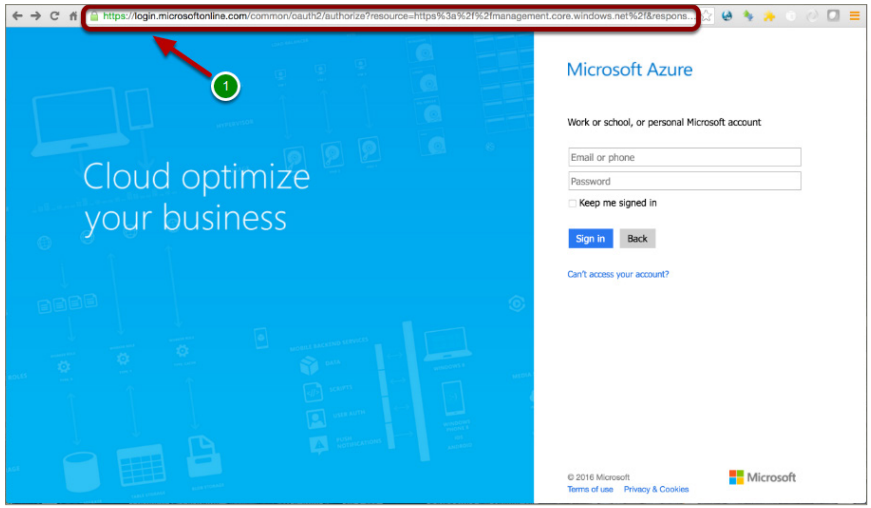
- Create a Microsoft Azure account
- Obtain a license (choose one of the following):
    1. Purchase a FortiGate Next-Generation Firewall license for Microsoft Azure http://www.windowsazure.com/en-us/account/
    2. Register to receive an evaluation license from Fortinet https://support.fortinet.com/Evaluation/Login.aspx

Step-by-Step Instructions to Get the FortiGate Up and Running on Azure

The following section will take you through a step-by-step process in order to deploy a Single Instance FortiGate on Azure.

1. Log In to the Azure Portal
   - You can access the Azure portal using the following URL: https://portal.azure.com/
   - You will be redirected to: https://login.microsoftonline.com/ (abbreviated URL due to its length)

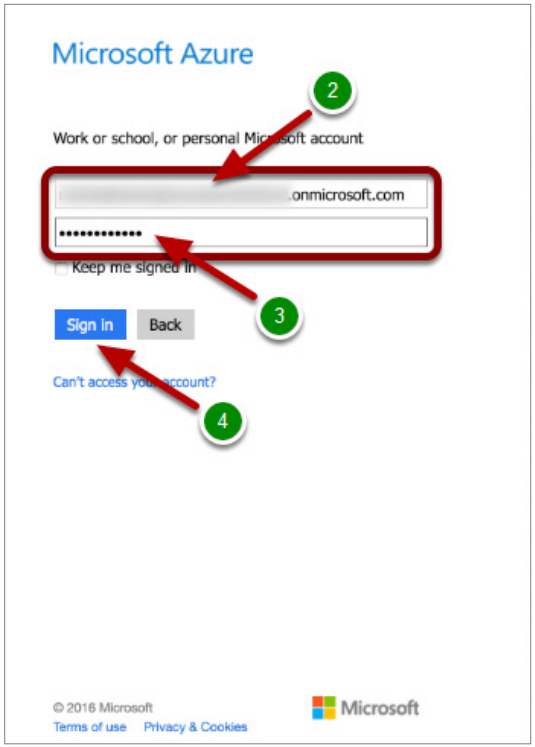
   The current Azure portal is the portal through which you will start creating and managing Azure services, such as the Fortigate NGFW Firewall Virtual Appliance. The Azure portal includes a dashboard that you can configure to work with and monitor the resources in your environment. The Azure portal lets you administer all of your Azure platform resources in a single location. The current Azure portal uses ARM, although some classic model functionality is exposed through the new portal. The legacy or classic portal still is available for use, but the new portal has been released for general availability and is the portal you should use.



2. Enter User Credentials and Sign In

   Enter your user credentials:

   - Username: <Your Username> (2)
   - Password: <Your Password> (3)
   - Click "Sign in." (4)

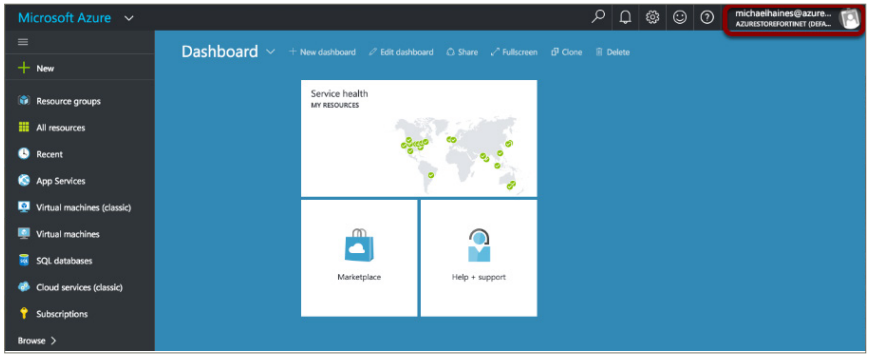


3. Successful Login to Azure

   Once you have successfully logged in to the Azure portal, you will observe the Microsoft Azure Dashboard.

   Note the following login details in the top right-hand corner of the Microsoft Azure Dashboard. If you click here, you will see options to:

   - Sign out
   - Change your password
   - View your permissions
   - View your bill

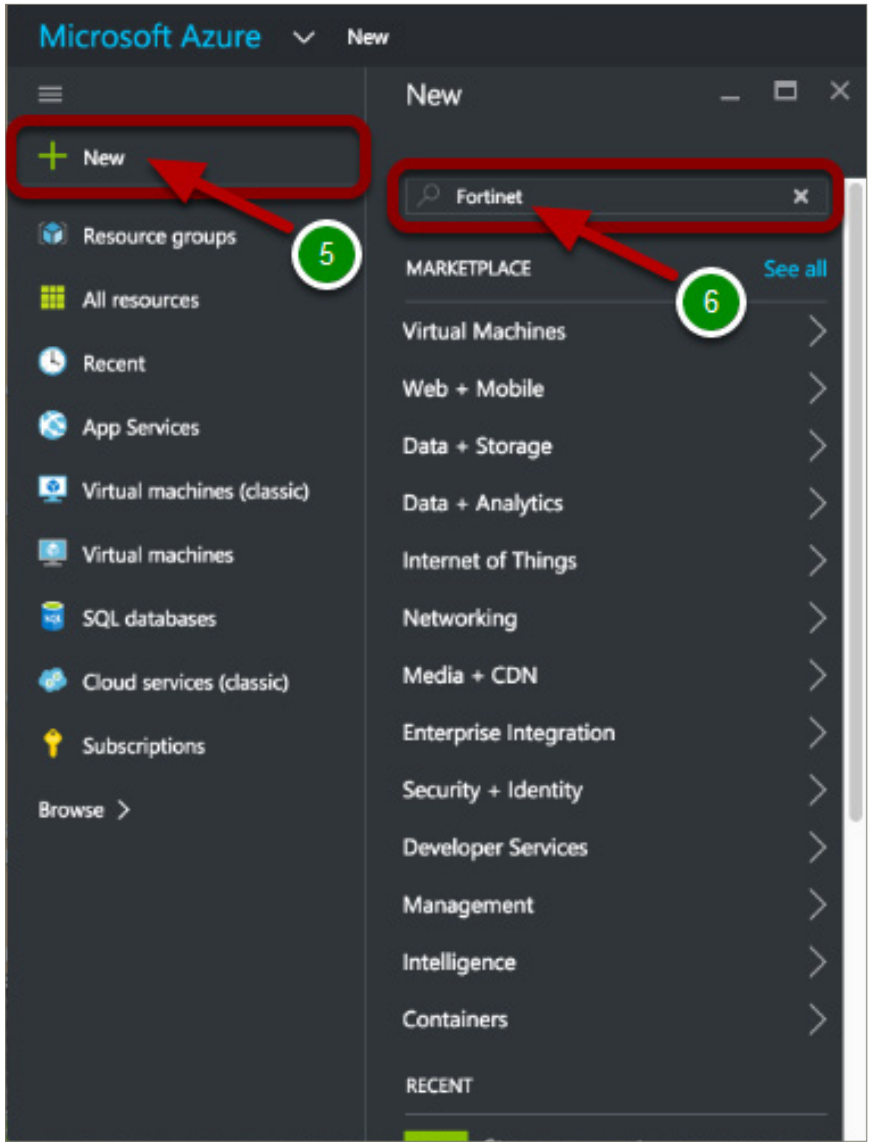


4. Creating the NEW FortiGate in the Azure Marketplace

   In the Microsoft Azure portal, follow these steps:

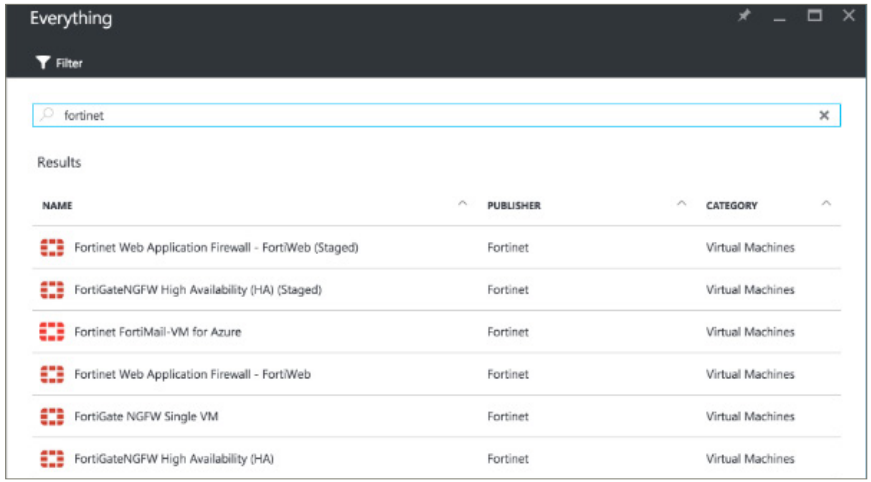
   - In the upper left-hand corner (5), click New.
   - In the New column, enter Fortinet in the "search the marketplace" and enter Return (6).

   NOTE: There are alternative ways of achieving the above; this is just one of the examples.



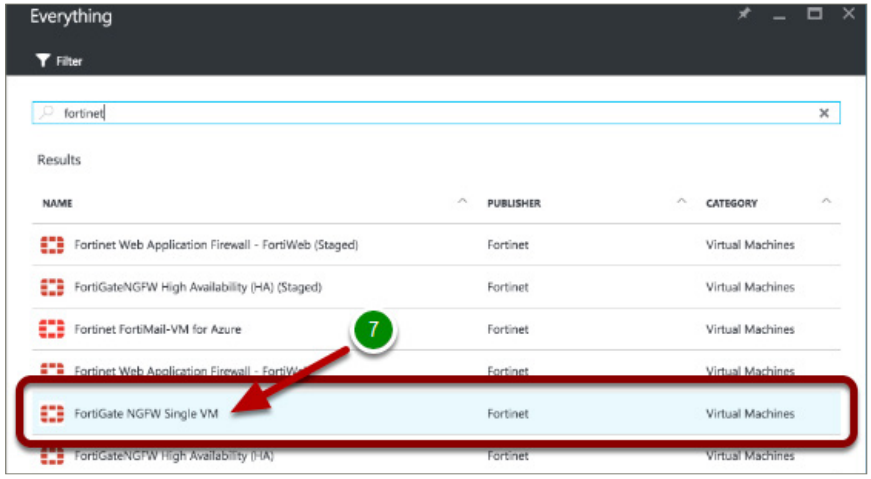
5. Fortinet Virtual Appliances Available in the Azure Marketplace

   You will now see something similar to this, which depicts the return of the "Fortinet" search results.



6. Select the FortiGate NGFW Single VM from the Azure Marketplace

   Select FortiGate NGFW Single VM (7).



7. Select the FortiGate NGFW Deployment Model

   Once you have selected the FortiGate NGFW Single VM, you will automatically be taken to the Resource Manager Panel, where you can create a deployment model.

   In the Select a deployment model, select the default Resource Manager (8).

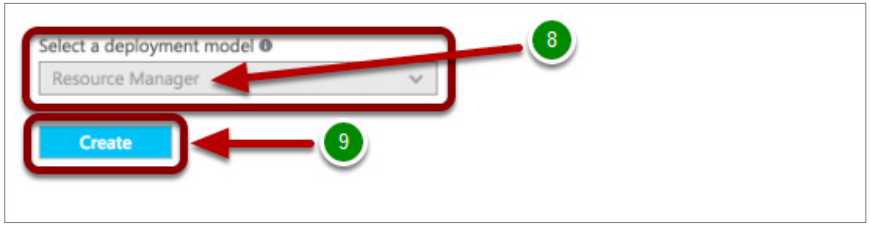
   Then click Create (9).

   NOTE: Though there is no option from the dropdown menu to select a different deployment model, this is where you would select the Classic deployment model option.

   So what exactly are the Azure deployment models?

   Azure provides two deployment models, the Classic model and the Azure Resource Manager (ARM) model. The foundation of each model is an application-programming interface (API), which is the Resource Manager API for ARM and the Service Management API for the classic model. Although developers can write software to interact with these APIs directly through the REST API, it is more common to interact with these APIs indirectly using the Azure portal, the Azure PowerShell on Windows, or the Azure Command-Line Interface (CLI) on a Windows, OS X, or Linux computer.

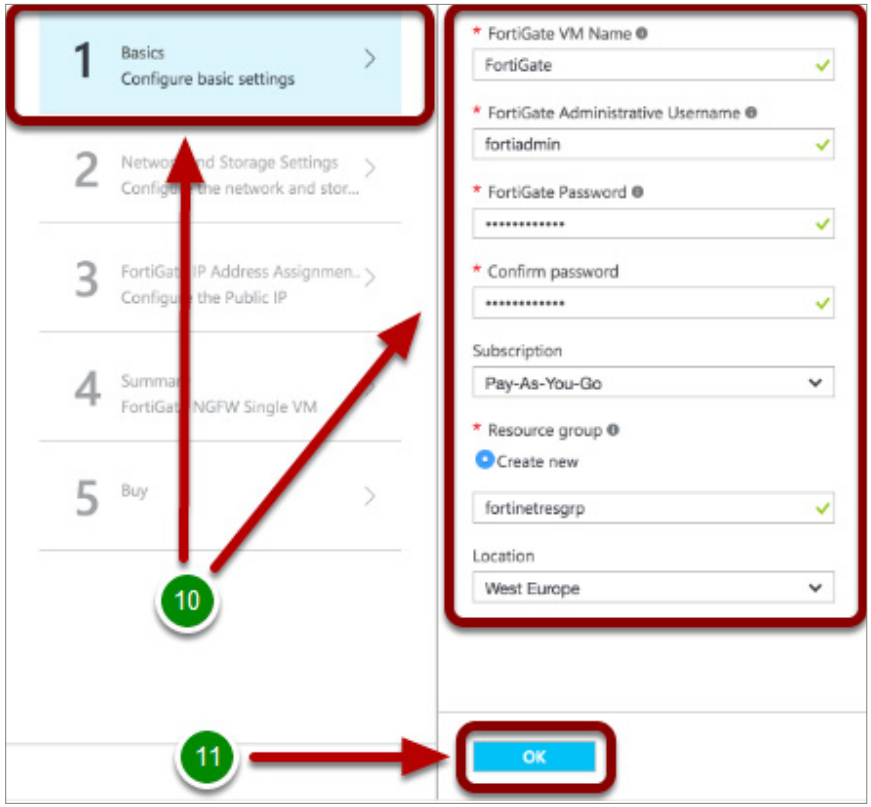
   In contrast to common belief, these two models are compatible with each other, but ARM simplifies the deployment and management of resources by managing them as a single resource group. Most newer resources support ARM, and eventually all resources will. However, how you create, configure, and manage Azure resources is different in these two models.



8. Configuring the FortiGate NGFW Basic Settings

   In the Configure basic settings panel (10), enter:

   - **FortiGate VM Name**—Enter the name of the FortiGate Virtual Appliance. (Only alphanumeric characters are permitted, and the value must be between 1 and 15 characters.)
   - **FortiGate Administrative Username**—Enter the administrator username for the FortiGate Virtual Appliance. (The administrator username for the FortiGate Virtual Appliance cannot be "admin.") If you do enter "admin," you will get an error message stating that the specified username is NOT allowed. In addition to this, the username can NOT contain special characters.
   - **FortiGate Password**—Enter the administrator account password for the FortiGate Virtual Appliance. (The administrator account password MUST be between 6 and 72 characters, and MUST contain characters from at least three of the following groups: uppercase characters, lowercase characters, numbers, and special characters.)
   - **Confirm password**—Re-enter the administrator account password for the FortiGate Virtual Appliance.
   - **Subscription**—The only available subscription for the FortiGate Virtual Appliance in Azure is the Pay-As-You-Go subscription model, so just leave this as "default".
   - **Resource group**—Enter the Resource group name, and note that only alphanumeric characters, periods, underscores, hyphens, and parentheses may be used. In addition to this, a Resource group name can NOT end with a "." (With Azure Resource Manager, everything you provision on Azure is a resource. You can put multiple resources into a resource group. Managing resource groups and creating and updating resource groups are the most common operations using Azure Resource Manager.)



- **Location**—Select a location from the drop-down menu. The location refers to allowing you to administer all of your Azure platform resources in a single location.

Once you have confirmed that all the above settings are correct, click "OK." (11)

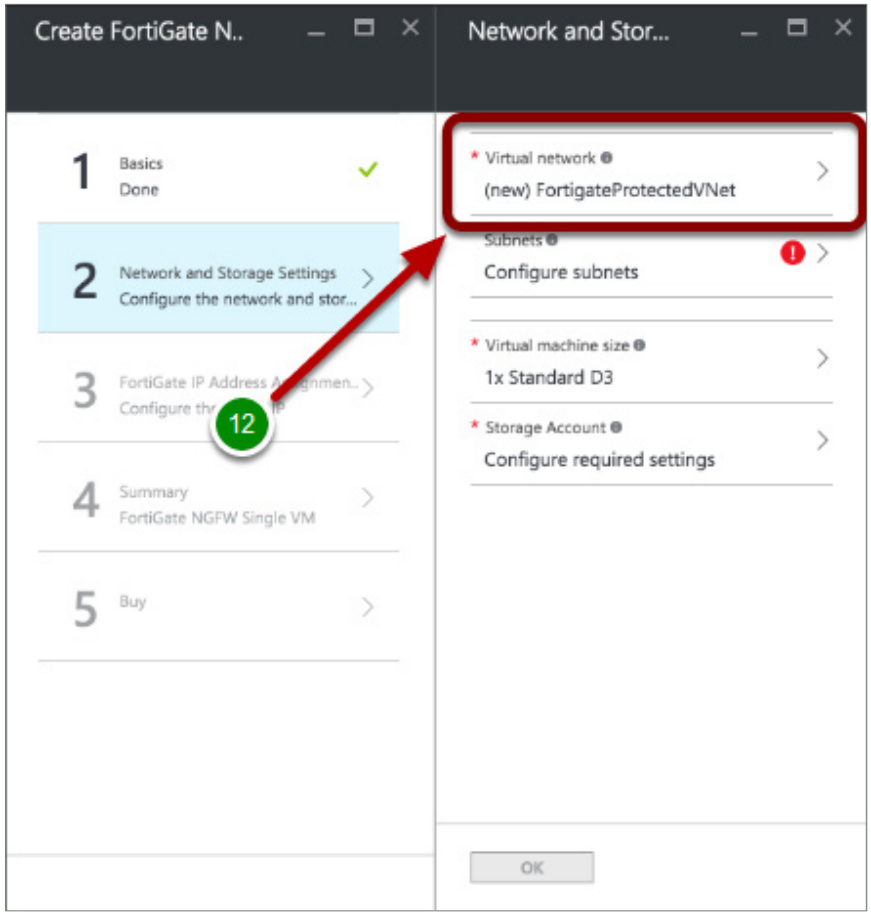
NOTE: If any of the values are incorrectly defined, you will see a "Red !"; otherwise, you will see a "Green ✓."

9. Configuring the FortiGate NGFW Network and Storage Settings

   In the Configure Network and Storage Options panel, we will look at each configuration option individually. Let us first start with what is presented by default when you select the Network and Storage Settings.

   As you can see, this is what is presented to you without any configuration changes that have yet to take place.

   Select the Virtual network settings (12).



10. Configuring the FortiGate NGFW Network and Storage Settings (Virtual Network)

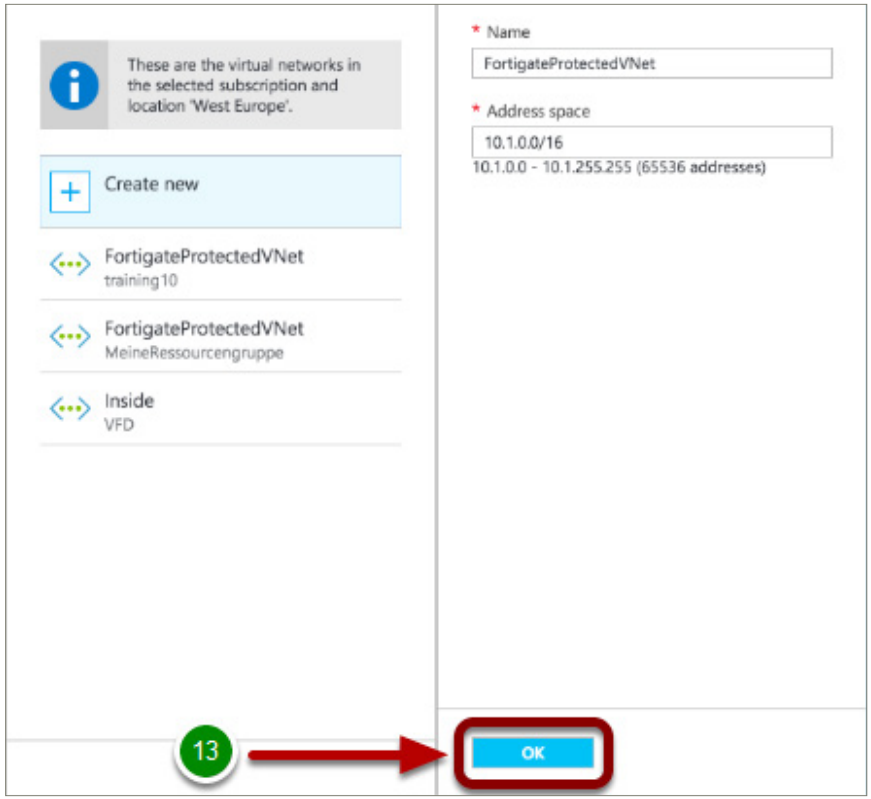
    The first question that comes to mind about a virtual network (VNET) is why do we need a VNET? Well, the answer is a simple one and the basic principle here is that we need a VNET in order to be able to build a private network in the Azure cloud.

    An Azure Virtual Network, which is also known or referred to as a VNET, is something that you only create in Microsoft Azure. The Azure Virtual Network enables virtual machines and the other resources that are part of the Azure Virtual Network to communicate with each other privately. It is the Azure Virtual Network that provides this communication function. If we did not have an Azure Virtual Network, or if a virtual machine was outside the Azure Virtual Network, then communication with other virtual machines would not be possible.

    After you have selected the Virtual network settings, you will observe that you can either create a new virtual network or select an existing one. If you select an existing virtual network, it will need to have at least two subnets in order for the FortiGate NGFW to route between them. In a typical deployment, the "outside" subnet just connects the FortiGate outside interface to the Azure Public Load Balancer and therefore does not need to be very large.

    Here you are just going to accept the default Virtual network name of FortigateProtectedVNet and the Address space of 10.1.0.0/16. Click OK (13).

    NOTE: No changes have been made here.



11. Configuring the FortiGate NGFW Network and Storage Settings (Subnets)

    Virtual networks in Azure are logically isolated from one another. In a VNET, you configure the IP address ranges, subnets, route tables, gateways, and security settings in a similar manner in your own data center. Virtual machines within the same VNET can by default communicate with one another. Connectivity from outside the virtual network, such as from within Azure or from the Internet, to a virtual machine requires a private or a public IP address.

    After you have selected the Subnets settings, you can also observe that you already have the following subnets defined:

    - Outside Subnet name: PublicFacingSubnet
    - Outside Subnet address prefix: 10.1.0.0/24
    - Internal Subnet name: FortigateInternalSubnet
    - Internal Subnet address prefix: 10.1.1.0/24

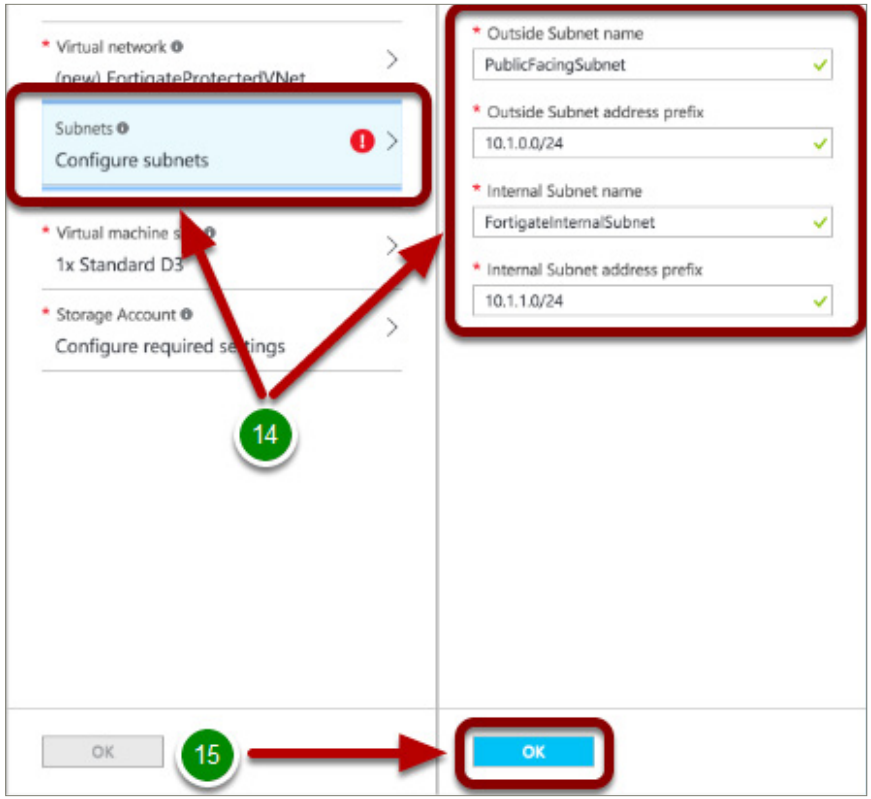
    The Outside and Inside address fields are prepopulated with the first useable address in the subnet (Azure uses the first four addresses in each subnet). However, if deploying to an existing subnet, this address may already be in use.

    So how does the IP addressing work? When a virtual machine is deployed into a VNET, its internal IP address is assigned from the subnet you specify and is dependent on the order in which it was provisioned, unless a static IP has been specified. For example, the FortigateInternalSubnet subnet created uses the address prefix of 10.1.1.0/24. The first four IP addresses of each subnet are reserved. With this knowledge in hand, it is easy to deduce that the first IP address available in this subnet will be 10.1.1.5. Unless otherwise specified, a virtual machine will be assigned the next available IP address from the subnet to which it was assigned at provisioning time.

Select the Configure subnets settings (14).

Here you are just going to accept the default Subnets configuration and click OK (15).

NOTE: No changes have been made here.



12. Configuring the FortiGate NGFW Network and Storage Settings (Virtual Machine Size)

    In the Azure Marketplace, the FortiGate virtual machines come in a variety of sizes, beginning with the D2 series with two cores up through the D4 series virtual machines with up to eight cores. Each virtual machine size within each series has different limits for the amount of memory, number of NICs, maximum number of data disks, size of cache, maximum IOPS and bandwidth, and maximum network bandwidth.

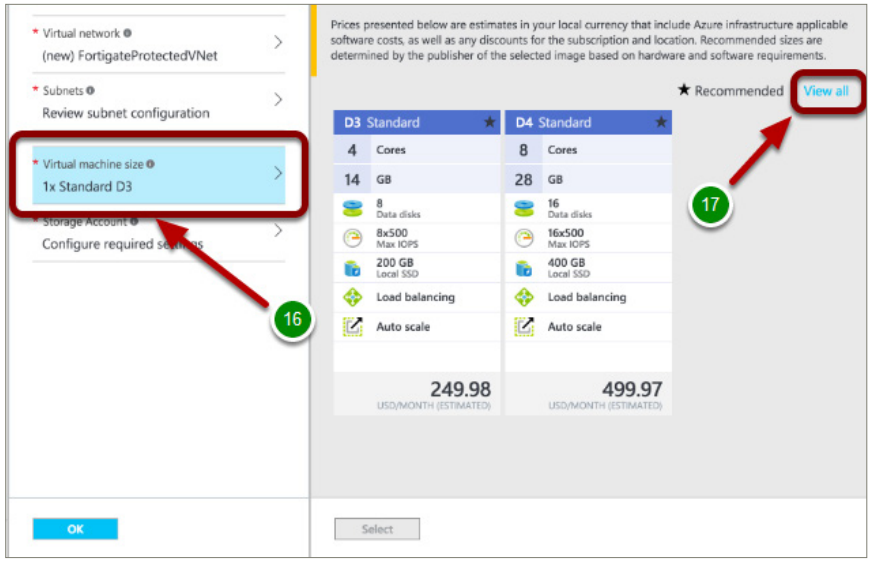
    Select the Virtual machine size settings (16).

    Select the View all setting (17).

    After you select the View all setting, you will be presented with all the available FortiGate virtual machine sizes, which include:

    - A4 Standard
    - D2 Standard
    - D3 Standard
    - D4 Standard
    - D2_V2 Standard
    - D3_V2 Standard
    - D4_V2 Standard

    So what are “A4 Standard” and “D4 Standard?” Number of vNICs? What would be the use case for selecting the particular “virtual machine size?” Where can you find more guidance, so when you are selecting and setting this up you are more informed.



The “A4 Standard” and “D4 Standard,” etc., are what are referred to as instance sizes. The instances are differentiated primarily on CPU and memory, although they also have different levels of support for multiple vNICs. For more information, please click on the following URL:

https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-sizes/

But wait! When you select a “virtual machine size,” why do you not see the number of vNICs? From the “choose a size” panel, you have no idea and would have to guess. The answer is that Azure has never prioritized multiple vNICs. So, the Azure Marketplace templates have a bias against them, and it’s extremely difficult to create a variable number of vNICs. So, all templates in the Azure Marketplace are static at two vNICs.

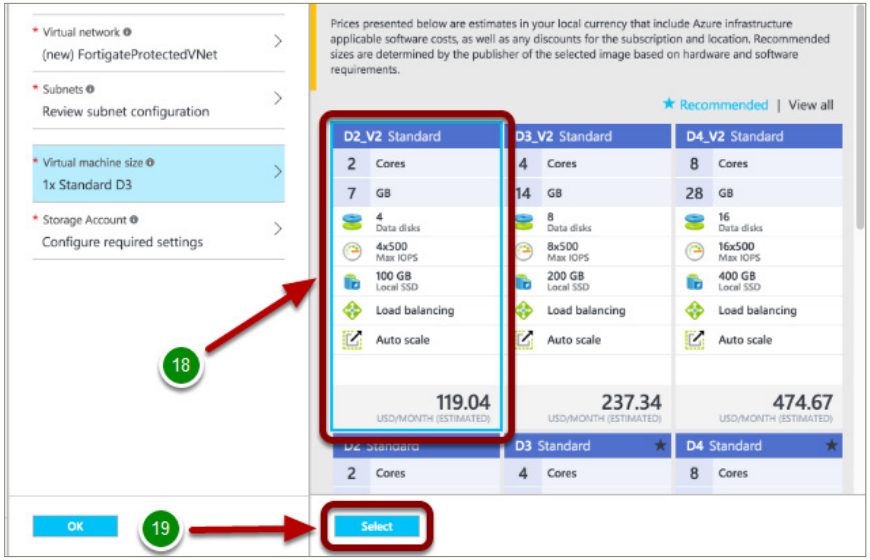
If you require more than two vNICs, you will need to deploy a custom template at this point. Please contact the Azure team (azuretech@fortinet.com) for assistance.

12a. Configuring the FortiGate NGFW Network and Storage Settings (Virtual Machine Size)

In this example you are going to select and use the D2_V2 Standard instance size.

Select the D2_V2 Standard instance size (18).

Then click Select (19).



13. Configuring the FortiGate NGFW Network and Storage Settings (Storage Account)

    Without going into the details of the different types of storage available in Azure, it is important to note (there are few exceptions) that all storage types are created from an Azure Storage Account. The Azure Storage Account in turn determines certain characteristics for the storage, such as whether the storage is locally redundant or geo-redundant, and whether the storage is based on standard HDDs or SSDs.

    You can either create a new storage account or select an existing one for the FortiGate Virtual Appliance, but all resources should be in the same location (in this example: West Europe).

    Select the Storage Account settings (20).

    Enter a Storage Account Name (21). (This account name can contain lowercase characters and numbers, and must be between 3 and 24 characters.)

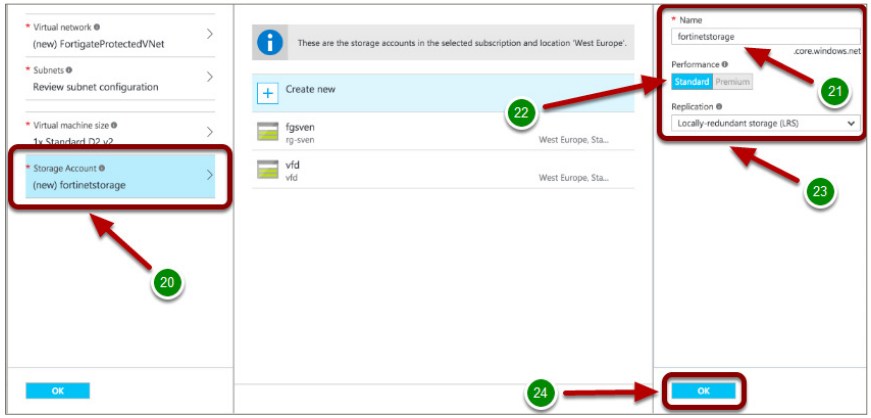
    Select the Performance (22). (In this instance only standard is available.)

    Select the Replication option you wish to use (23). There are two options available:

    - Locally redundant storage (LRS)
    - Geo-redundant storage (GRS)

    Locally redundant storage (LRS) is where all data in the Azure Storage Account replicates synchronously to three different storage nodes within the primary region that was chosen when creating the Azure Storage Account.

    Geo-redundant storage (GRS) is where every entity is replicated into two data centers.



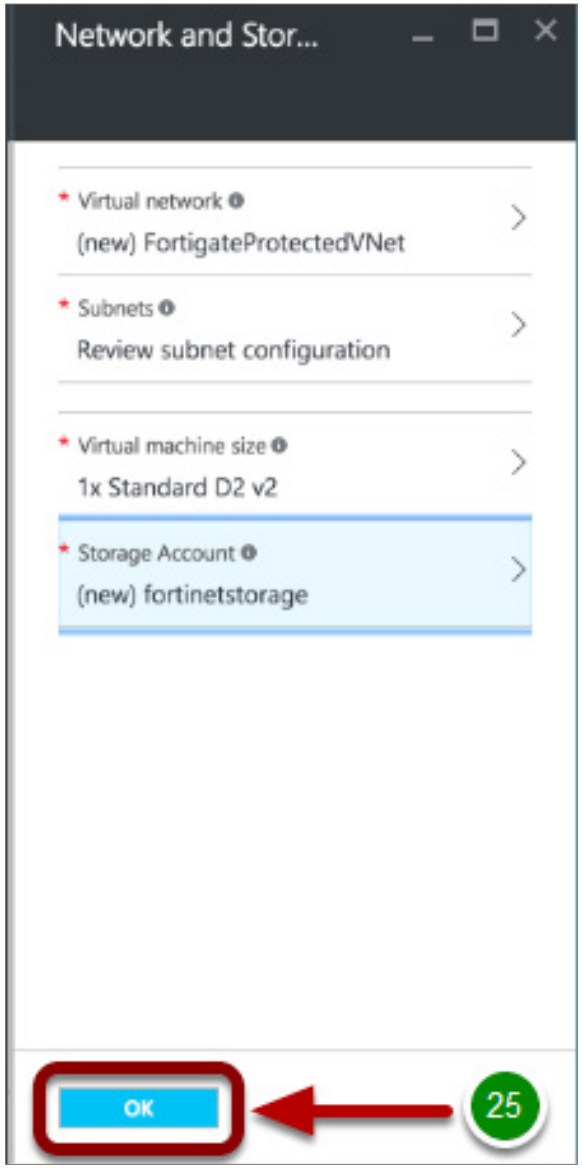
The data in the Azure Storage Account is always replicated in order to ensure durability and high availability. Be aware that some settings cannot be changed after the storage account has been created.

Select OK (24).

14. FortiGate NGFW Network and Storage Settings (Completed)

    After successfully completing the FortiGate NGFW Network and Storage Settings, you should see something similar to the above.

    Select OK (25).

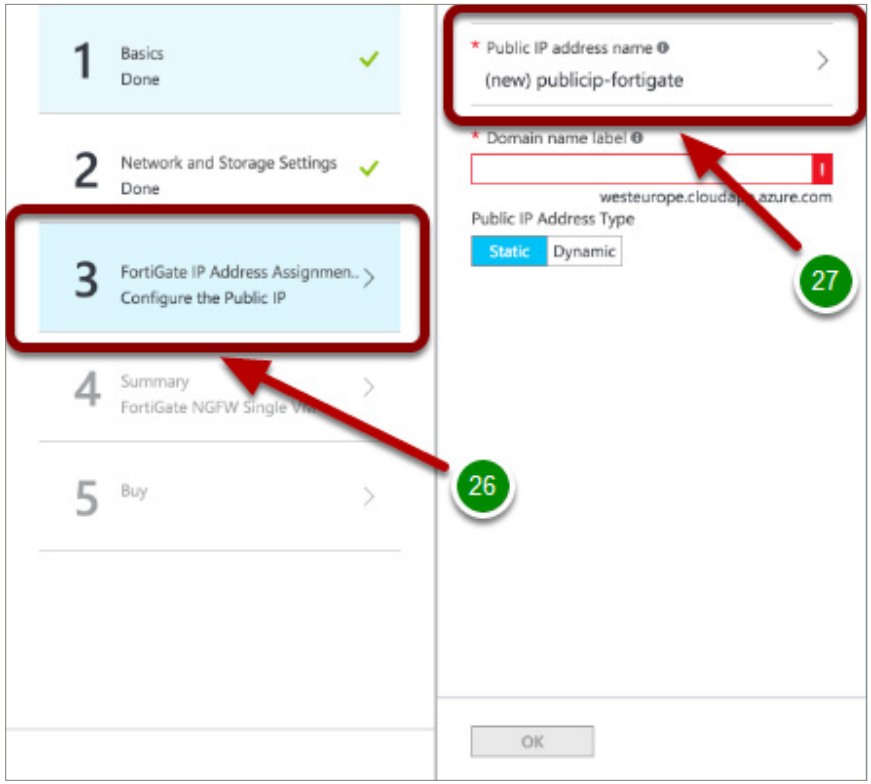


15. Configuring the FortiGate NGFW IP Address Assignments Settings (Public IP)

    Select the FortiGate IP Address Assignments Settings (Public IP) panel (26).

    Select the Public IP address name (new) publicip-fortigate settings (27).

    NOTE: Don't worry about Domain name label and Public IP Address Type, as this will be covered next.



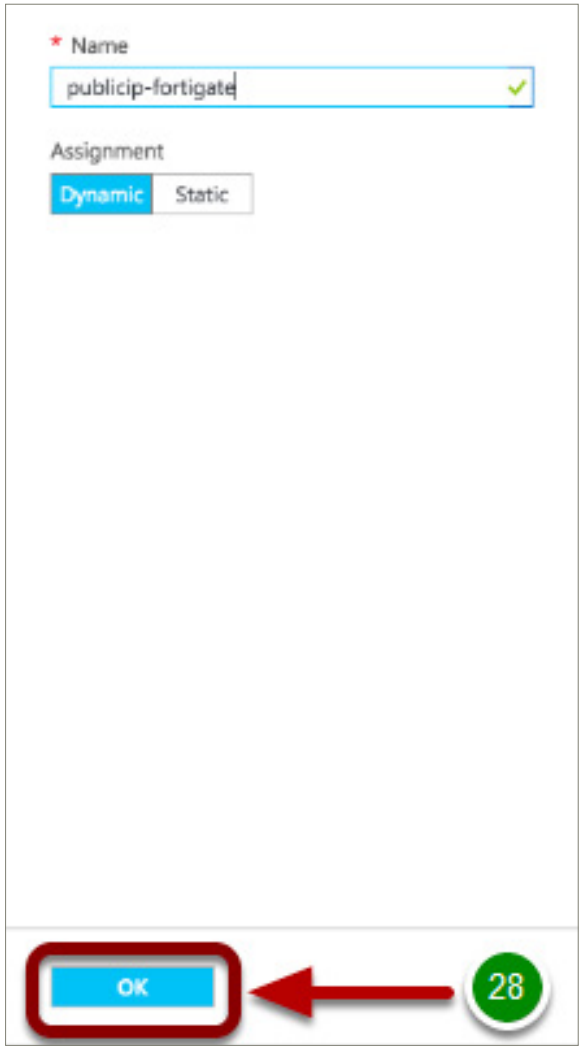
15a. Configuring the FortiGate NGFW IP Address Assignments Settings (Public IP Address Name)

This is where you can set the Public IP Address Name and the Assignment to either Dynamic or Static.

You will leave these as default.

Select OK (28).

NOTE: No changes have been made here.



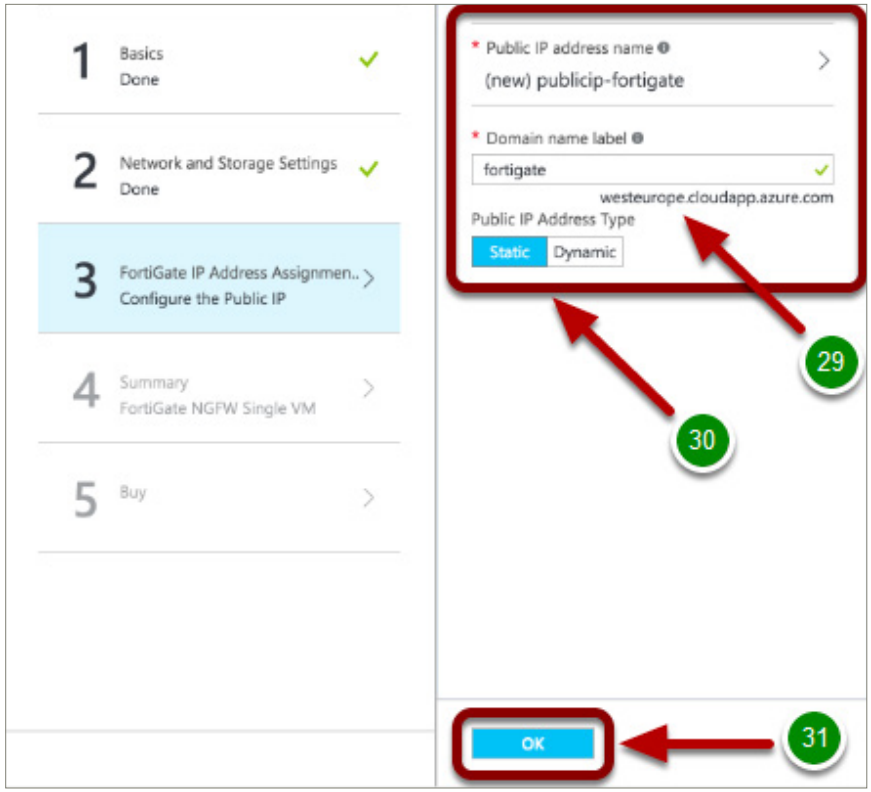
15b. Configuring the FortiGate NGFW IP Address Assignments Settings (Domain Name)

Next, you need to enter a valid DNS Domain Name Label (which is a DNS prefix). This will be used for the Public IP Address.

- Enter a Domain name label (29).
- Select either a Static or Dynamic Public IP Address Type (30).

In the Public IP Address Type, a “Static” Public IP Address will be reserved across reboots and shutdown states, while a “Dynamic” address will be reassigned.

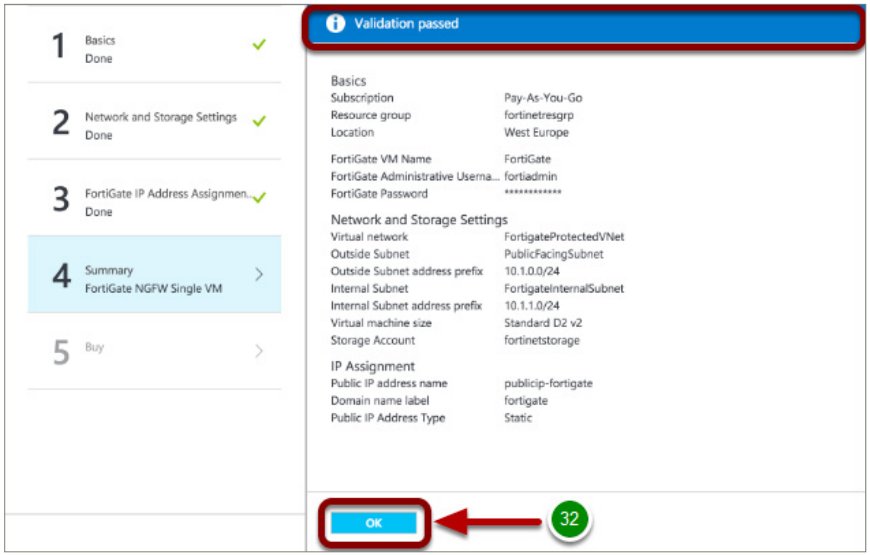
Select OK (31).



16. FortiGate NGFW Single VM (Summary)

    After selecting “OK,” a validation process will take place and your configuration will be validated. If successful, you will see Validation passed.

    Select OK (32).

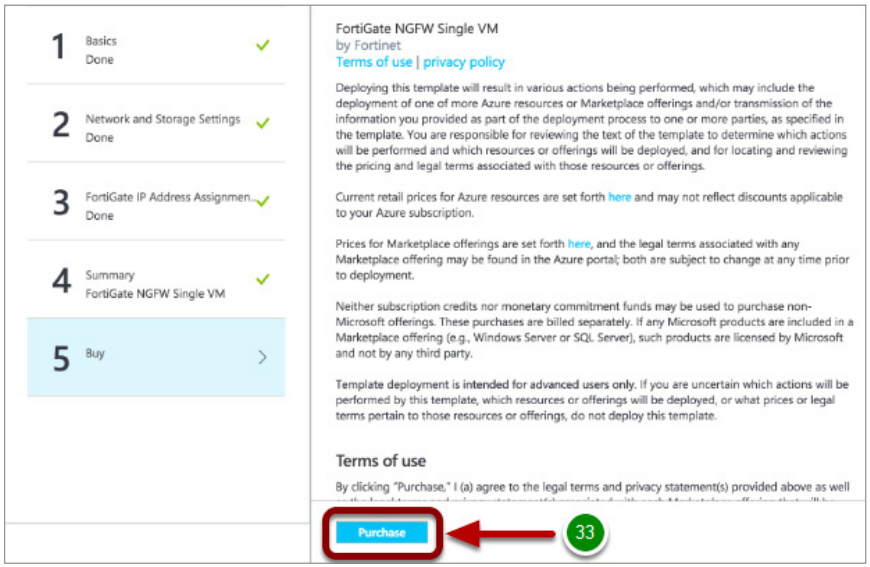


17. FortiGate NGFW Single VM (Purchase)

    After the FortiGate NGFW Single VM Configuration has been completed, you now are required to select “Purchase.”

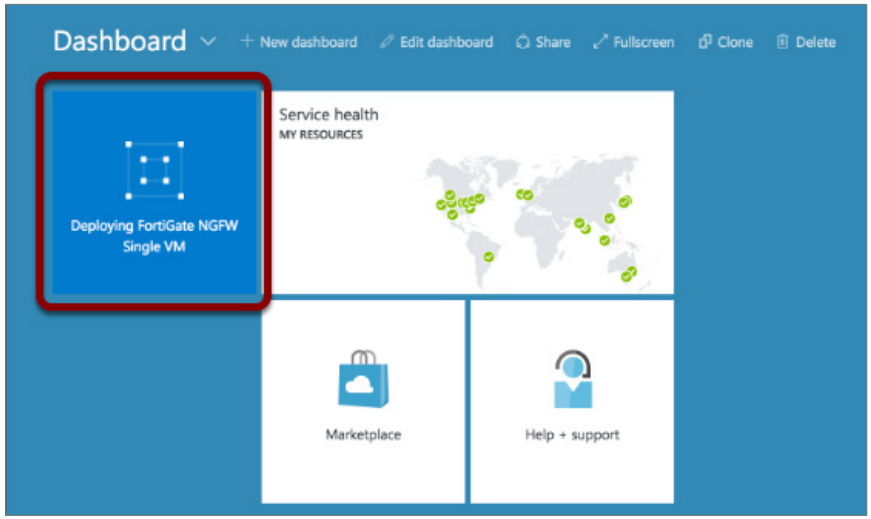
    Select Purchase (33).

    NOTE: Purchase just means that you are going to be paying Azure for the virtual machine use time. You still must obtain a license separately from Fortinet, Inc.



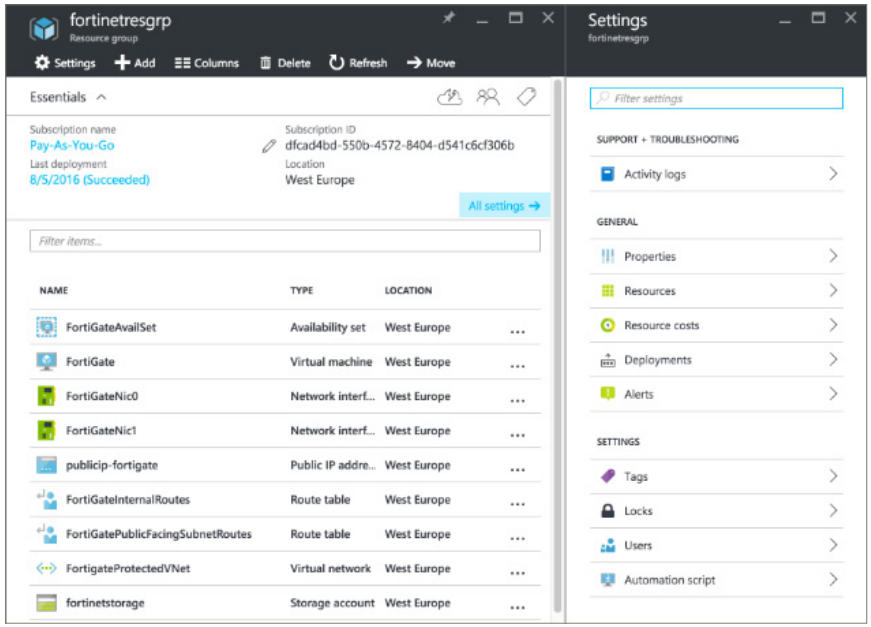
18. FortiGate NGFW Single VM (Deploying)

    After selecting “Purchase,” the FortiGate NGFW Single VM will be deployed. This process can take approximately 10 minutes to complete, but may vary depending on location and number of resources being requested.



19. FortiGate NGFW Single VM (Deployed)

    After the FortiGate NGFW Single VM has been deployed, you will be redirected to a screen similar to this which shows all the resources that have been instantiated by the template.



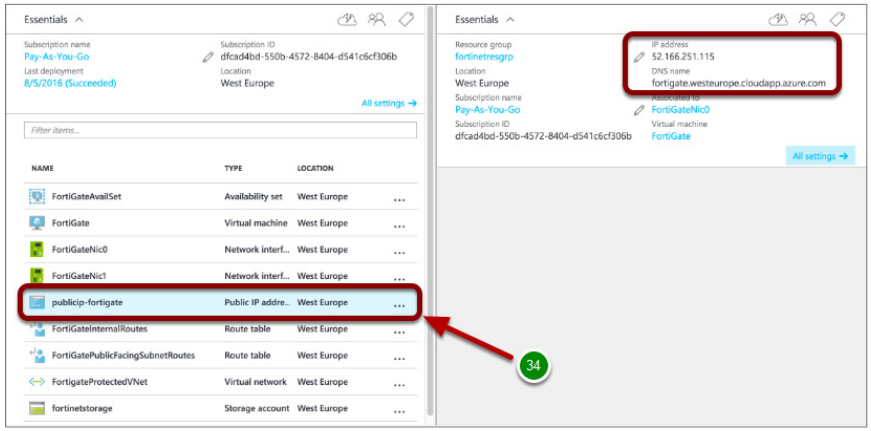
20. FortiGate NGFW Single VM Accessible Public IP Address

    In order to be able to connect to the FortiGate Public IP Address, you need to know what this IP address is.

    To accomplish this:

    Select the public IP resource to get your DNS name or public IP address (34).

    This will expose the Public IP Address, which is 52.166.251.115, and a DNS of fortigate.westeurope.cloudapp.azure.com.



21. Basic IP Communication with the FortiGate NGFW Virtual Appliance (ping)

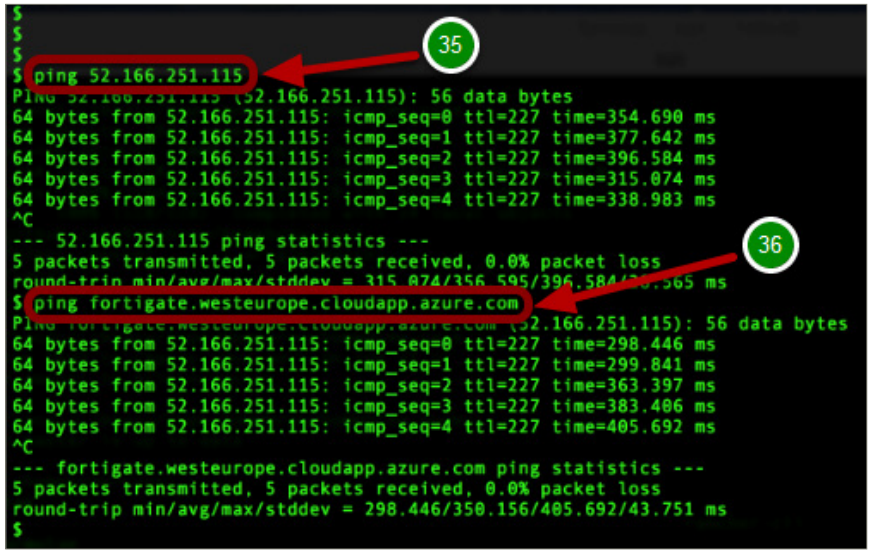
    Now that you have the Public IP Address, you can connect to your Azure FortiGate Virtual Appliance either via HTTPS or SSH.

    Before you do that, let's initiate some basic IP connectivity and confirm that you can indeed communicate with the FortiGate Virtual Appliance.

    In the following steps, you will use ping (8) to resolve both the IP Address and Name Resolution.

    Use the ping (8) utility (35) to ping the IP Address 52.166.251.115.

    Use the ping (8) utility (36) to resolve the DNS name of fortigate.westeurope.cloudapp.azure.com.

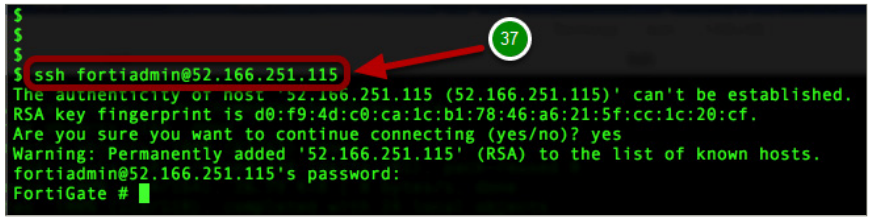


22. Basic IP Communication with the FortiGate NGFW Virtual Appliance (ssh)

    In the following step, you will use ssh (8) to connect to Fortigate NGFW IP Virtual Appliance.

    Use the ssh (1) utility (37) to connect to the IP Address 52.166.251.115.

    NOTE: Or you could use the DNS name.



23. Connect to the FortiGate NGFW Virtual Appliance UI

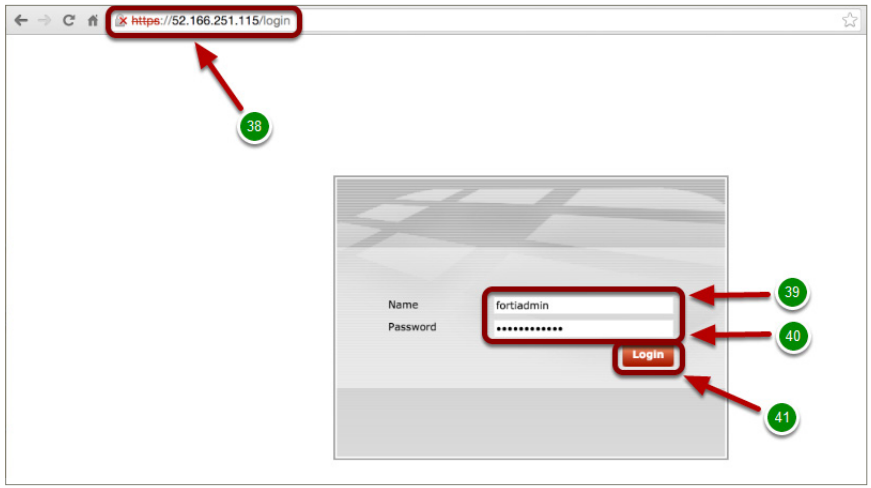
    Now that you have confirmed that you have IP communication to the FortiGate NGFW Virtual Appliance in Azure, you can connect to the UI using HTTPS.

    - Using your favorite browser (38), such as Firefox or Chrome, connect to the IP Address 52.166.251.115.
    - Enter the FortiGate Administrative Username (39).
    - Enter the FortiGate Administrative Password (40).
    - Select Login (41).

    Recall in Step 8 you defined both the username and password, which are as follows and are required to connect to the FortiGate NGFW Virtual Appliance UI:

    - FortiGate Administrative Username: fortiadmin
    - FortiGate Password: <the password you entered>

    NOTE: The template also redirects ports 500, 4500, and 1701 to the FortiGate in order to support VPN connections.



24. License Your Azure FortiGate NGFW Virtual Appliance

    Upon a successful login, you will be redirected to the following URL:

    Currently our Azure Marketplace deployment only supports BYOL. This means you will need to purchase Azure-specific licenses for the appliance you are going to deploy.

    NOTE: If you have a mismatch between the VM size and the license (i.e., more CPUs assigned to the VM than are licensed), you will receive an error message, and the FortiGate configuration will not be available.

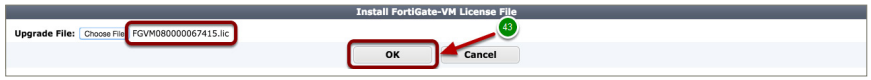
25. Install the FortiGate VM License File

    Select Choose File (42).

25a. Install the FortiGate VM License File

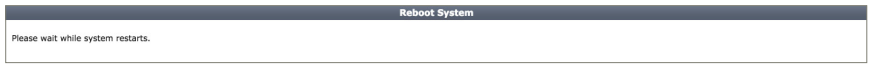
    Here you can see the selected License File: FGVM080000067415.lic.

    Select OK (43).



25b. Rebooting the System

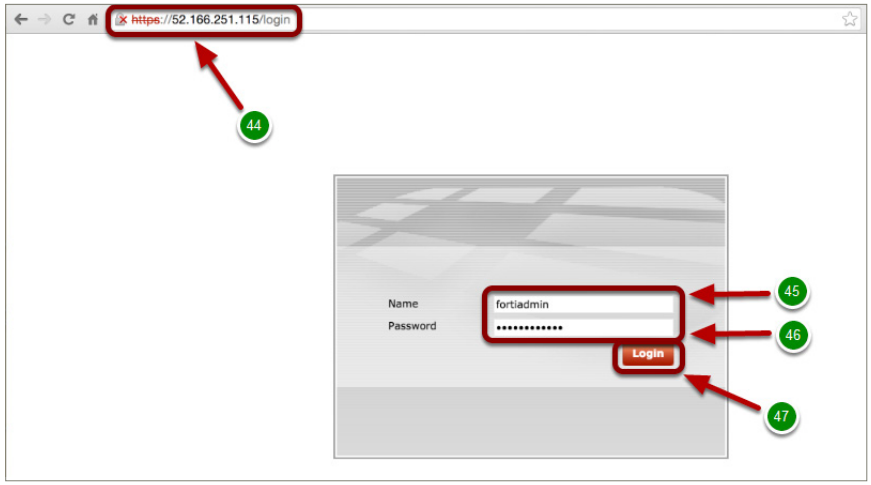
    Once you have selected the license file, you will then be informed that the system is being rebooted.



26. Log In to the FortiGate NGFW Virtual Appliance UI

    After the system reboot has been completed, log back in to the FortiGate NGFW Virtual Appliance UI.

    - Using your favorite browser (44), such as Firefox or Chrome, connect to the IP Address 52.166.251.115.
    - Enter the FortiGate Administrative Username (45).
    - Enter the FortiGate Administrative Password (46).
    - Select Login (47).



27. FortiGate NGFW Authentication and Registration

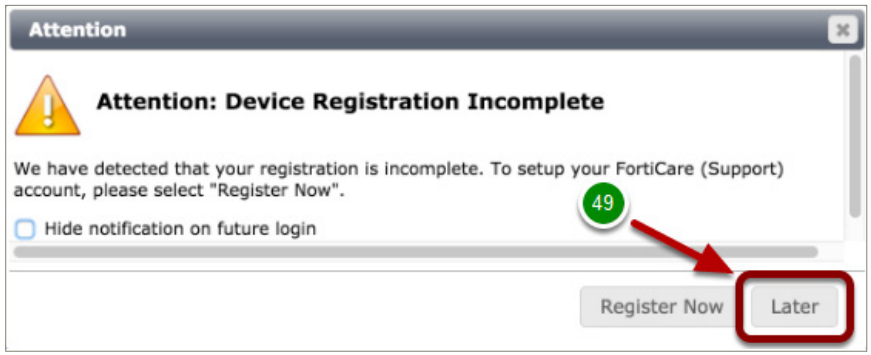
    Once you have successfully logged in, you will see that the license has been uploaded and you will need to wait for authentication with the registration servers. This can take a while (10-15 minutes or so), so please be patient.

    Select Return (48).

28. FortiGate NGFW Device Registration Incomplete

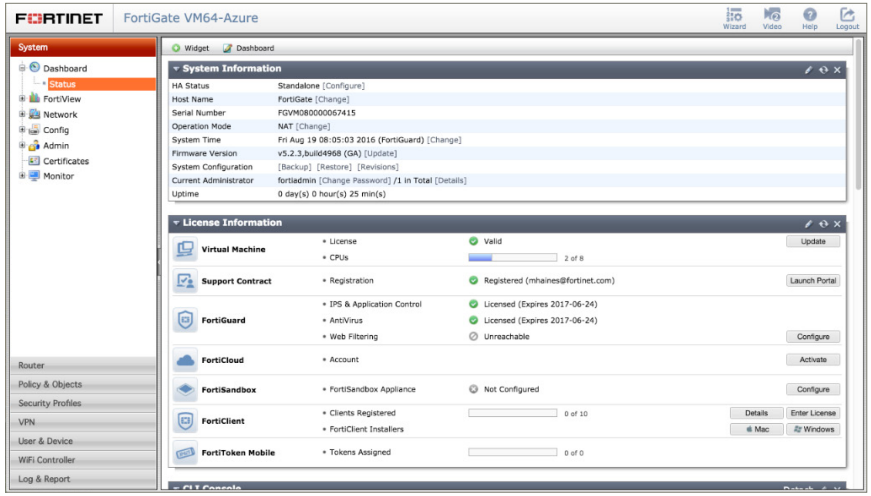
    If you see an alert message like the one shown above, please select “Later” and proceed.

    Select Later (49).



29. FortiGate NGFW Virtual Appliance UI Dashboard

    This is what a successful login looks like, and now you can see you have access to the FortiGate NGFW Virtual Appliance UI dashboard.



Support

For more in-depth instructions, please refer to http://docs.fortinet.com/ for administration guides or email your support questions to azuretech@fortinet.com.

v1.0 09.07.16